CHAPTER

10

DESIGNING SECURE ACCESS TO THE INTERNET

After reading this chapter and completing the exercises you will be able to:

- Understand how to secure an internal corporate network by implementing various security services, such as Network Address Translation, firewalls, and Demilitarized Zones.
- Secure user access to the Internet by implementing proxy services, such as Microsoft Proxy 2.0 and Internet Security and Acceleration Server 2000.
- Design and implement a corporate Internet usage policy.

The Internet has become one of the most important business tools for many companies. Just as the desktop PC has changed the way users do their work, the Internet is taking business to a new level of functionality and complexity. Corporations can now communicate and share information almost instantaneously with people anywhere in the world. Business partners can share many online services, such as inventory or customer databases. Consumers no longer have to purchase items during regular "store" hours. They can simply browse to a company Web site and purchase merchandise 24 hours a day, seven days a week.

Along with this convenience and efficiency comes the ever increasing concern over security. Almost everyone is aware of the Internet security issues, so for companies and consumers to feel safe conducting online commerce, security must have a high priority. Corporations are concerned that allowing resources to be available on the Internet increases the possibility of an attack on their internal network systems. Consumers are concerned about the security of information, such as credit card numbers or other personal information, when they conduct online transactions. If a company is going to be successful doing business on the Internet, security has to be a prominent component of the overall planning.

In addition to the compromise of information, there are many other types of Internet-based threats that can cause problems for a company. Companies that rely on the Internet cannot afford any downtime. Many online Internet companies have lost millions of dollars just because their services were not available to consumers for a relatively short period of time. In many cases, the downtime results from attackers causing various types of denial-of-service attacks to disrupt the regular flow of network traffic. For more information on the types of attacks that can occur, refer to Chapter 1, "Identifying Security Risks."

There are many Windows 2000 features that you can implement to help secure access to the Internet. The first part of this chapter discusses the components that you can use to ensure that the internal network is secure from external attacks. The initial design of the network infrastructure can assist in making the Internet more secure. Design plans that utilize features such as Network Address Translation or Demilitarized Zones (DMZ) should be part of the overall security strategy. Hardware-based or software-based firewalls placed between the internal network and the Internet can also assist in maintaining security. Even the basic task of keeping up with security patches and configuring security features, such as auditing or NTFS permissions, should be an essential part of the overall security plan.

The second section of this chapter explains various ways to secure user access to the Internet. If you allow uncontrolled and unprotected Internet access, you are exposing your internal network to several risks. One of the most common risks is the introduction of viruses into the corporate network. Other risks include attacks on internal computers and the use of infected computers in coordinated attacks against other networks over the Internet. Employee productivity can also be decreased because of personal rather than business Internet usage or the use of corporate computers for fraud, pornographic, or other types of illegal activity.

To assist in making user access to the Internet secure, administrators can plan and deploy services, such as a proxy server or firewall. Proxy servers, such as Microsoft Proxy 2.0 or Internet Security and Acceleration Server 2000, provide many proxy and firewall-based features. These tools can be used to control and report Internet usage for both inbound and outbound access.

Many companies also implement an Internet usage policy to ensure that employees understand what is acceptable with regards to Internet usage within the company. The last section of this chapter will discuss the topics that should be included in the design of an effective corporate Internet usage policy.

Securing the Internal Network from the Internet

When a connection to a public network, such as the Internet, exists, network administrators inherit the additional responsibility of securing the internal network from attack. Most attacks are launched against common Internet servers, such as Web or e-mail

servers. Several steps can be taken to ensure that these services, as well as the internal network, are secure from Internet-based attacks.

The first step in securing these servers is to analyze the service components that are exposed to the Internet. In most cases, the only services that you want to have directly accessible from the Internet are web servers or e-mail servers. Many of these "front-end" components connect to back-end servers, such as database or file servers. As you design your Internet security plan, you must examine each component and server that is accessible from the Internet as a potential target for attack and design your security plans to remedy these threats.

Simple tasks, such as making sure that the network services have the latest service and security patches, can greatly assist the administrator in keeping the network secure. For example, in the summer of 2001, the infamous Code Red Worm infected thousands of IIS servers throughout the world. This happened despite constant warnings and notifications for administrators to apply an available patch that would have fixed the problem. It is very important for administrators to take security warnings seriously or be ready to work overtime to repair infected servers.

To assist you in keeping up with all of the latest security issues and fixes, you can subscribe to the Microsoft Security Notification Service at *http://www.microsoft.com/technet/security/notify.asp*. The security advisor sends automatic notifications of security issues by e-mail.

Another step towards internal network security is to disable all of the server services that are not required. For example, Windows 2000 installs Internet Information Services by default. Any machine, including almost all workstations, that is not sharing Web-based information, should have IIS uninstalled. Other services, such as Telnet or even the Server Service (for workstations), should be evaluated to see if the network has a need for the particular component. This requirement is especially important for any server that is directly connected to the Internet. For example, if you leave the Server service enabled on an Internet-connected server, anyone on the Internet can easily view all of the share names that you have created on the server. A basic rule is that, on Internet connected servers, you should disable all the network services except for the ones specifically required for the server.

If you are using Internet Information Services (IIS) 5.0 as your Web server, you also have to plan for IIS security. Many default settings in IIS 5.0 are not considered secure. For example, the ftproot and mailroot directories have the Everyone group assigned with full control. These permissions should be tightened depending on the level of functionality needed.

Other basic security measures that should be applied to an IIS 5.0 server include the following:

- Set appropriate Access Control Lists on all virtual directories on the IIS server.
- Configure and monitor logging on the IIS server.
- Set appropriate permissions on the IIS log files to prevent malicious users from deleting the log files to cover their tracks.
- Disable or remove all sample applications from a production server, such as the IIS Samples and IIS Documentation information.
- Be sure to remove the IISADMPWD virtual directory if the server has been upgraded from IIS 4.0. This directory allows the resetting of Windows NT and Windows 2000 passwords and should not be installed on a Web server.

For more information on securing and locking down both IIS 4 and 5 Web servers, access the Microsoft Security Tools Web site at *http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/ tools/tools.asp*.

E-mail servers, such as Exchange 5.5 or 2000, should also be considered in the security plan. Almost all companies now have an SMTP server that is directly accessible from the Internet, so this server must also be protected. You should adopt many of the same practices for these servers as you would with your Web servers. Microsoft frequently releases security and service patches to fix discovered vulnerabilities and bugs. These service patches should be applied to remedy these bugs.

The most common security breach related to e-mail servers is the transmission of virus-infected e-mail. Antivirus scanners should be installed, not only on the client workstations but also on the e-mail server, to enable the interception of viruses before they infect the workstations.

An effective security plan not only involves the security of the individual network services but also includes the initial design of the network infrastructure. Network design plans that include services such as NAT, firewalls, and Demilitarized Zones (DMZs) can greatly enhance security for a corporate network. The next sections discuss these concepts in greater detail.

Network Address Translation

One of the goals of a comprehensive security plan is to protect the internal network IP addressing scheme. If the internal addresses become known, an attacker can attempt an IP spoofing attack by sending packets which seem to originate from the internal side of the network. Likewise, if the internal IP addresses of file or database servers are discovered, attacks can be attempted to corrupt, steal, or deny service to these locations. Network Address Translation (NAT) can be used as a method of concealing internal network addresses.

Network Address Translation (NAT) protects a network by replacing the source internal address and ports of all outgoing packets with a single public IP address. When the internal clients connect to the Internet, the NAT device keeps track of all connections so that any returned packets can be routed to the correct internal destination on the network. In addition to providing security by hiding the source address, this service also enables many connections to share a single outbound connection to the Internet. The internal addressing scheme of the network commonly uses **Request for Comment (RFC) 1918** addressing. This RFC states that certain IP addressing ranges have been designated as private and will connect to the Internet only through NAT devices. The private IP address ranges include:

- 10.0.0.0–10.255.255.255
- 172.16.0.0–172.31.255.255
- 192.168.0.0–192.168.255.255

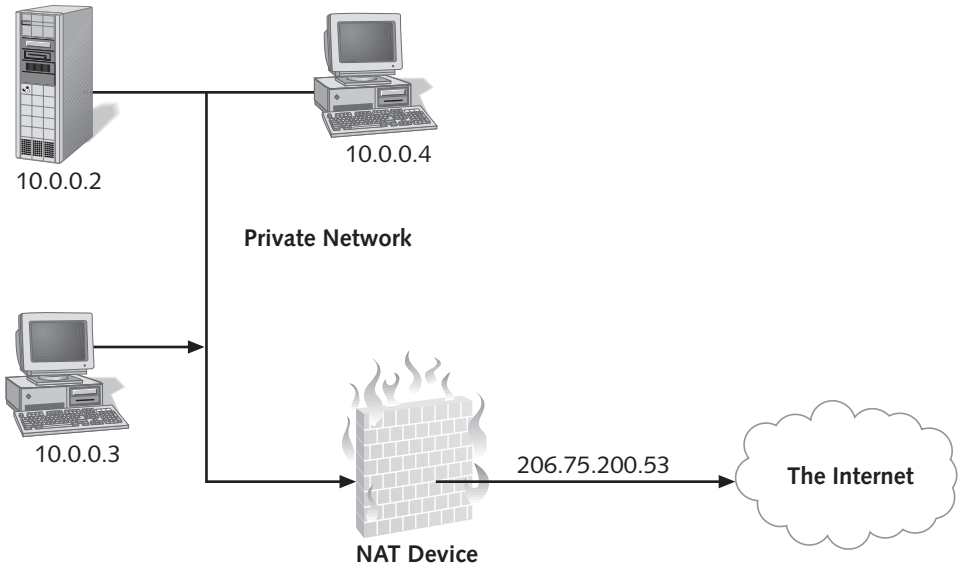
The NAT device usually incorporates two network adapters. One adapter is connected to the private network and is assigned a private IP address, the second adapter is connected to the Internet with a public IP address assigned by an Internet Service Provider.

Figure 10-1 illustrates a NAT device in use. When the client with the internal address of 10.0.0.3 accesses the Internet, the source IP address is translated to the public IP address 206.75.200.53. If the client is connecting to a Web server, for example, the packets being sent to the Web server would have a source address of 206.75.200.53, and the Web server would send packets back to this address. When the packets arrive at the NAT device, the destination address is translated to 10.0.0.3 and sent to the internal client. The same process takes place when the 10.0.0.4 client accesses information from the Internet.

Windows 2000 provides two components that can function as NAT devices: Internet Connection Sharing, and Routing and Remote Access.

Internet Connection Sharing (ICS)

Windows 2000 Server and Professional include a component called **Internet Connection Sharing (ICS)**. ICS is a very simple Network Address Translation device that allows the sharing of a single Internet connection to multiple workstations within a network. This component is quite useful for small office or home-based networks, as it is easy and quick to configure. To configure ICS, all you have to do is share an Internet connection. To make the configuration of your network even easier, ICS includes a simple DHCP server that automatically assigns addresses from the private IP address range of 192.168.0.0 to internal client machines.



Source IP	NAT Translated IP
10.0.0.3	206.75.200.53
10.0.0.4	206.75.200.53

Figure 10-1 Internal hosts accessing the Internet through a NAT device

In most cases, ICS will be configured on a computer with two network cards, one connected to the Internet, and one connected to the internal network. The card that is connected to the Internet is configured with the information supplied by the Internet Service Provider. The card connected to the internal network then provides the gateway to the Internet for the internal clients.

To configure Internet Connection Sharing, follow the procedure below.

1. Right-click **My Network Places** and click **Properties**.
2. Right-click the network adapter that is connected to the Internet connection (e.g., cable or DSL modem) and click **Properties**.
3. Click the **Sharing** tab and click **Enable Internet Connection Sharing for this connection** as shown in Figure 10-2. Click **OK**.

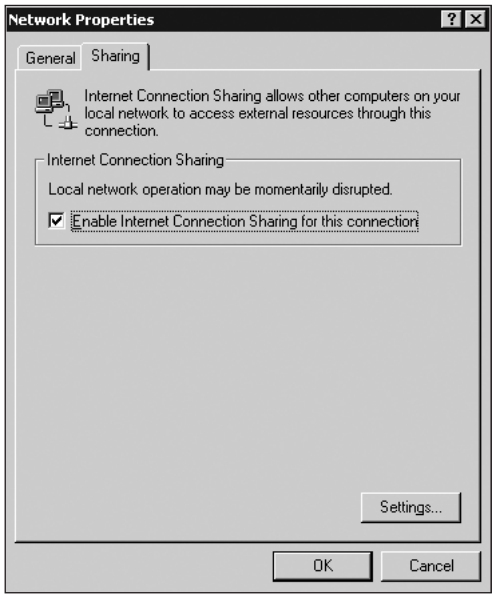


Figure 10-2 Enabling Internet connection sharing

4. A message box appears stating that ICS will set the adapter connected to the LAN to use IP Address 192.168.0.1. (See Figure10-3.) It also states that other computers attached to the LAN should be set to obtain their IP Addresses automatically. Click **Yes** to enable Internet Connection Sharing.

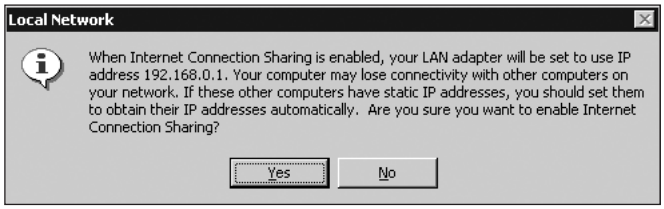


Figure 10-3 Internet connection sharing warning message

Many companies will not implement Internet Connection Sharing because of the strict limitations ICS imposes on the configuration of the NAT services. For example, ICS does not allow you to turn off the DHCP services or to change the 192.168.0.0 range. This may not work well with companies that use a different internal addressing scheme or that already have a DHCP server in place. Also, you cannot change the IP address for the internal network card. For companies that require the benefits of a NAT device, but also require more functionality, Windows 2000 Server includes a more advanced NAT device in its Routing and Remote Access Services.

Routing and Remote Access Services

As stated in Chapters 8, "Securing Access For Remote Access Users" and 9, "Securing Access Between Corporate Locations" Windows 2000 RRAS consists of many individual subservices. Included in these components is the capability of providing full-featured NAT. The advantages to using the RRAS version of NAT is that all the RRAS security features, such as policies and packet filtering, can be applied to the NAT server. You also have the option of enabling or disabling a NAT-based DHCP server to accommodate companies that may or may not have a DHCP server already in place. In addition, you are not restricted to using only IP addresses in the 192.168.0.0 range. You can use any IP addresses internally, and require only one valid Internet address.

To configure a NAT server using RRAS, follow the steps below:

1. Open **Routing and Remote Access** from the **Administrative Tools** menu.
2. If RRAS has not been set up, right-click the server name and choose **Configure and Enable Routing and Remote Access**.
3. The RRAS Wizard will start. Click **Next**.
4. In the **Common Configurations** screen, click **Internet Connection Server**, and then click **Next**.
5. The **Internet Connection Setup** screen will prompt you to choose between ICS or NAT. Choose **NAT**, and then click **Next**.
6. On the **Internet Connection** screen, choose the network adapter that is directly connected to the Internet. If you are connecting with a dial-up modem or ISDN connection, choose to create a demand-dial connection. (The next step assumes that you have chosen a direct network adapter.)
7. Click **Next** and then click **Finish**. RRAS will start with the Network Address Translation service configured with the default settings. An illustration of the configured RRAS console is shown in Figure 10-4.

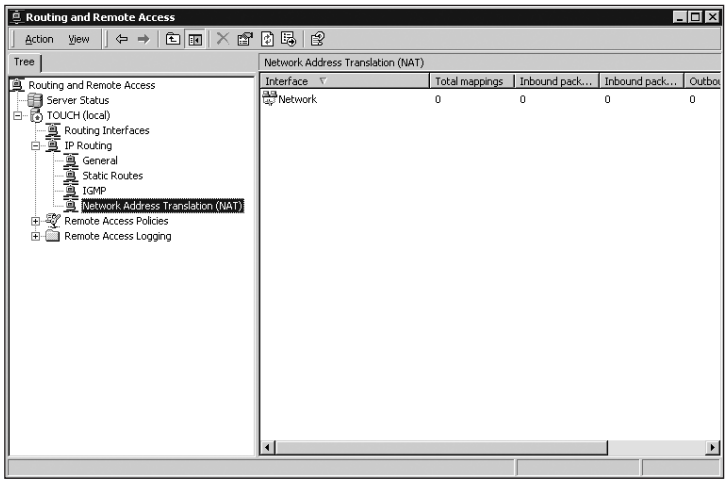


Figure 10-4 Configuring RRAS as a NAT server

In addition to the RRAS security features discussed previously in Chapters 8 and 9, there are many advanced NAT features that can be utilized within the RRAS console. These features include:

- Address Assignment (DHCP) options
- Incoming Session Mapping
- Various usage statistics, such as DHCP and DNS allocator information
- A list of all translated NAT sessions

To access features, such as DHCP options and usage statistics, right-click the NAT node on the left pane of the RRAS console. The list of translated NAT sessions and configuration of incoming Session mapping can be accessed by selecting the NAT node and then right-clicking the interface adaptor in the rightmost details pane as shown in Figure 10-5.

Configuring Firewalls

Another way of protecting the internal network from Internet attacks is to deploy a firewall. A **firewall** can be either a software-based or hardware-based component that is deployed between the Internet and the internal network and is configured to allow only specific types of traffic to pass from one network to the other. Usually the firewall is the single connecting point between the internal network and the Internet. By using a firewall, the administrator can control and monitor all incoming and outgoing network traffic. An example of a basic firewall configuration is shown in Figure 10-6.

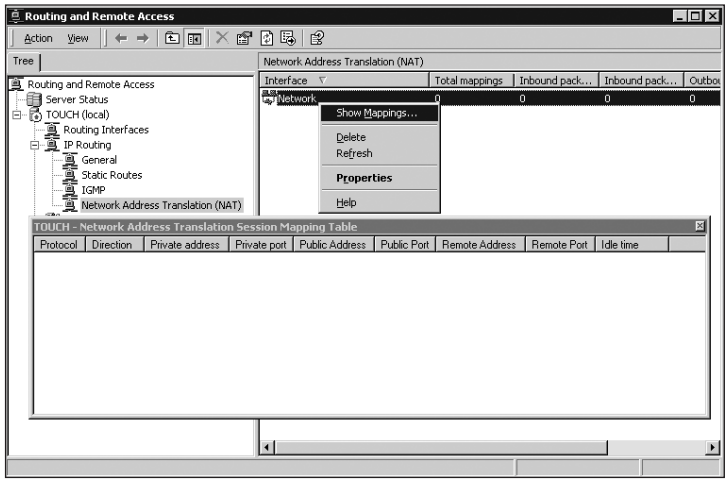


Figure 10-5 Viewing the NAT Session Mappings table

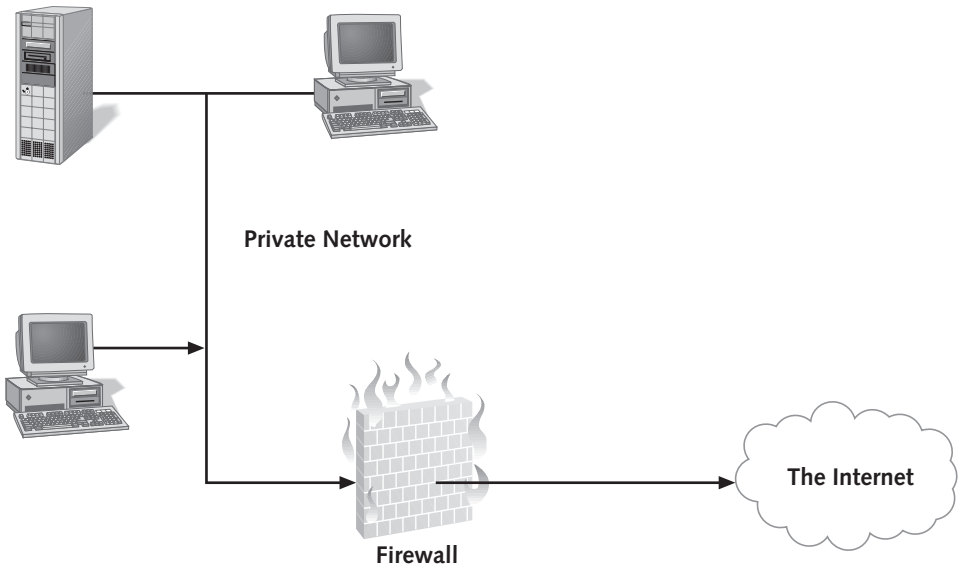


Figure 10-6 A firewall separating a private network from the Internet

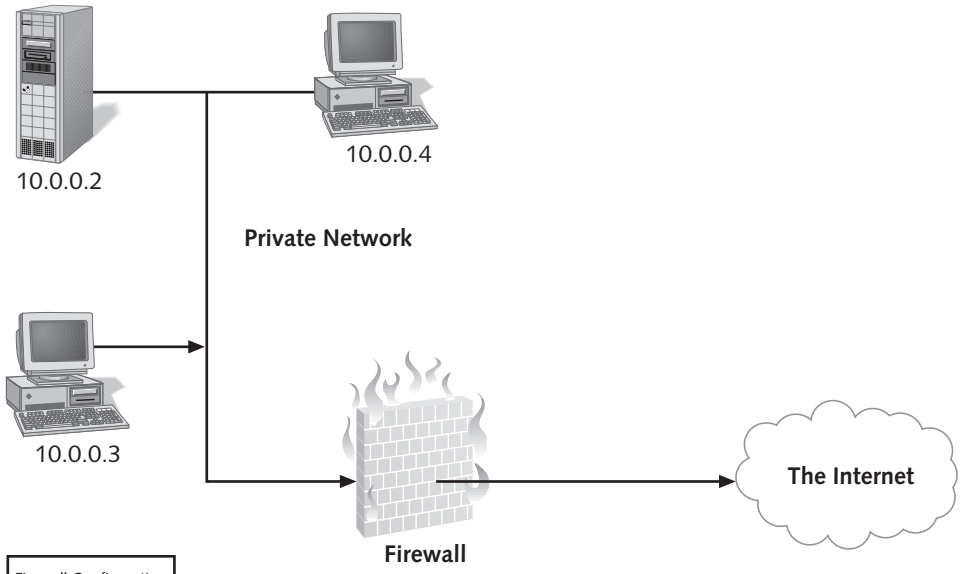
Most corporate-level firewalls offer a variety of features to assist in increasing the security of the internal network. In addition to NAT features, additional advanced features include:

- Packet Filter capabilities
- Reverse Proxy (static) mappings
- Advanced usage reports and intrusion detection

Packet Filtering

A **packet filter** is used to allow or deny access through a firewall. The packet filter is a set of rules describing the characteristics of the packets that will be forwarded across a firewall and the packets that will be blocked. These characteristics include packet attributes, such as source IP address, source port, destination IP address, destination port, and the transport protocol used. After each packet description, the packet filter defines whether to allow or disallow the packet transmission.

For example, if the Lonestar Graphics' security requirement allowed the passing of HTTP traffic through the firewall and a denial of any other type of protocol, the typical firewall configuration might be as shown in Figure 10-7.



Firewall Configuration

Order	Source IP	Source Port	Target IP	Target Port	Allow or Deny?
1	Any	TCP 80	Any	TCP 80	Allow
2	Any	Any	Any	Any	Deny

Figure 10-7 Firewall rule configured to allow HTTP traffic

Figure 10-7 illustrates that there are two packet filters set up on the firewall. The first packet filter states that any HTTP traffic (TCP Port 80) is allowed to pass through. The second packet filter denies all other traffic from crossing the firewall.

The combination of multiple packet filters is called a **firewall rule**. Most firewalls also feature a configuration setting that allows the administrator to mirror the firewall rule to ensure that response packets can be returned to the original source. In other words, you can configure a firewall rule allowing inbound HTTP traffic, and then mirror the rule to also allow outbound HTTP traffic. This saves on the number of packet filter entries needed to allow both inbound and outbound traffic to pass.

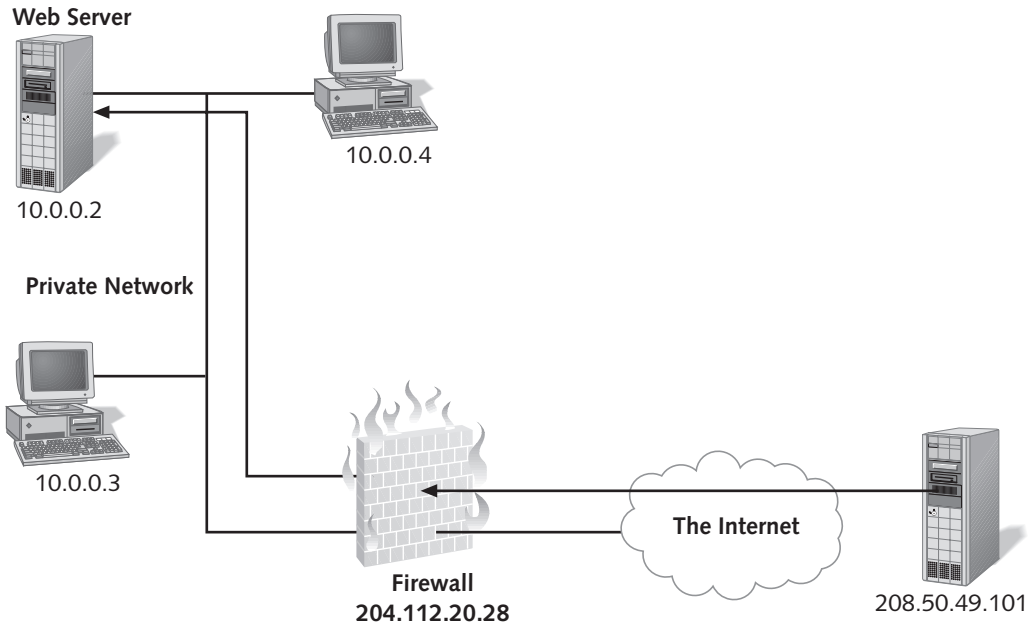
When you design the firewall security, you have a choice of two strategies that you can use to apply firewall rules. The first strategy is to deny all protocols and create additional packet filters that explicitly allow specific protocols. This strategy is most common within highly secure networks. Each allowed packet filter would be listed in order, with the last filter denying all other protocols from crossing the firewall. When a packet arrives at the firewall, the firewall evaluates each firewall rule in the order they are listed. If the packet characteristics match one of the firewall rules, the action associated with the rule is applied. If the packet characteristics do not match any of the firewall rules, then the last rule in the list explicitly denies the packet access.

The second strategy is to allow all protocols and explicitly deny prohibited protocols. This strategy is usually followed with networks that do not require high security. Each denied packet filter would be listed in order, with the last rule stating that any other packets not explicitly defined are allowed to cross the firewall.

For a list of which port numbers are used by which network services, check out the Web site: *http://www.iana.org/assignments/port-numbers*.

Reverse Proxy Mappings

Reverse proxy mappings (or static mappings) are configuration settings that direct incoming traffic to a particular resource located behind the firewall. For example, as Figure 10-8 illustrates, Lonestar Graphic's web server with a fully qualified domain name of *http://www.lonestar.com* is located behind the corporate firewall. With the assistance of DNS, this host name is converted to the public IP address 204.112.20.28, which is actually the IP address of the external network adapter on the firewall. When a request for the web server reaches the firewall, a configuration setting on the firewall states that any requests on port 80 should be redirected to server 10.0.0.2 using port 80.



Source IP	Target IP	Port	Mapped IP	Mapped Port
208.50.49.101	204.112.20.28	TCP 80	10.0.0.2	80

Figure 10-8 Static mapping configuration on firewall

The reverse proxy is used to protect the internal network as well as the server that is providing the service to the Internet. The firewall protects the internal network by redirecting all packets that match the rule to a single server inside the network. In this example, all HTTP packets will be redirected to the server with the IP address of 10.0.0.2. You can set up another Web server as an Intranet server for the internal network, but that server will not be accessible from the Internet. The firewall also protects the server that is providing the Internet service because the server is not directly exposed to the Internet. For example, you might set up a firewall to forward all SMTP traffic to an internal Exchange server. The Exchange server is not directly exposed to the Internet; the only access to the server from the Internet is through port 25.

Advanced Usage Reports and Intrusion Detection

Many firewall applications include extensive reporting capabilities to assist you in monitoring Internet usage, as well as monitoring intrusion attempts. Reports that may be available include:

- **Web Usage Reports**—Usually consist of top Web user statistics and top sites visited.
- **Application Reports**—Usually consist of top Internet application usage to assist in bandwidth and network capacity planning.
- **Traffic and Utilization Reports**—Include statistics relating to average traffic and peak simultaneous connections, proxy cache hit ratios, and total Internet usage by application, protocol, and direction.
- **Security Reports**—List possible attempts to breach security by identifying source IP address information (if known) and the type of attack.

Most firewall devices can also be configured to alert you in the event of a firewall attack. Firewall configurations can detect common attacks such as port scans, out-of-band attacks, or the ping-of-death. You also have the option of configuring what the firewall should do when it detects an attack. In some attacks, you may want to have the firewall shut down all access to the internal network. In other cases, you may want to have the firewall send an alert or e-mail informing you of the attack. This functionality is critical for a firewall. It may take a significant amount of time for an attacker to break through your firewall and gain access to your network. The firewall should be able to detect the intrusion attempt and send you an alert so that you can deal with the attempt, possibly before the attacker can actually gain access to the network.

Implementing Demilitarized Zones

Many companies provide multiple network services such as e-mail servers, Web servers, DNS, terminal services, and FTP servers that are accessible from the Internet. For many companies, providing these services on the Internet is an essential part of doing business. However, the more services that are made available to the Internet, the more difficult it is to protect the internal network from attack.

A common approach to protecting the internal network is to create a protected area between the internal network and the Internet using firewall technology. This protected area is known as a **Demilitarized Zone (DMZ)** or **screened subnet.** Any resources that are accessible from the Internet are placed within the DMZ. This design concept can help to ensure security because, if any of the resources within the DMZ become compromised, the internal firewall would still protect the corporate network from attack.

There are two main design strategies when planning the use of a DMZ: configuring a three-homed firewall DMZ or configuring a back-to-back DMZ.

Three-Homed Firewall DMZ

A **three-homed firewall DMZ** is a DMZ configuration in which a single firewall is set up with one network adapter connected to the Internet, a second adapter connected to the private network, and a third adapter connected to the DMZ. An illustration of this configuration is show in Figure 10-9.

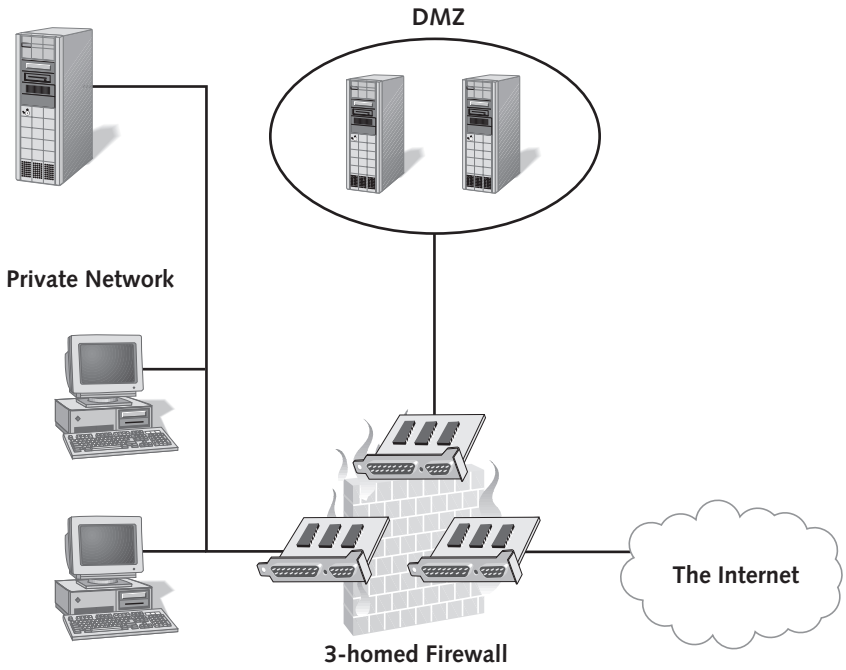


Figure 10-9 A three-homed firewall DMZ

In a three-homed firewall DMZ, the firewall rules direct traffic between the three interfaces. The internal network is protected since the rules make sure that all traffic coming from the Internet is directed only to the resources within the DMZ and is not allowed to enter the internal network. Additional rules may then be configured to allow some packets to flow from the DMZ to the internal network. For example, you may have a Web server in the DMZ that needs to access a database located in the internal network. To accomplish this, you would configure a rule on the firewall to allow traffic to pass from the Web server to the database server if the packet is using a specified port. The database server itself would not be accessible from the Internet because no traffic would ever flow from the Internet directly to the internal network.

When planning the design for a three-homed DMZ, connect each interface to its own segment. The DMZ segment can have either a public or private IP addressing scheme. If IPSec is going to be used to connect to the public network, you must use public IP addresses within the DMZ as IPSec will not work through a NAT server. Another consideration is that even though a three-homed DMZ may be less costly because only one firewall is being implemented, a security breach on the firewall may result in all of the network segments being exposed. In general, a three-homed DMZ is less secure than a back-to-back DMZ.

Back-To-Back DMZ

A **back-to-back DMZ** uses two firewalls to create a protected network segment between the internal network and the Internet. An example of a back-to-back DMZ is shown in Figure 10-10.

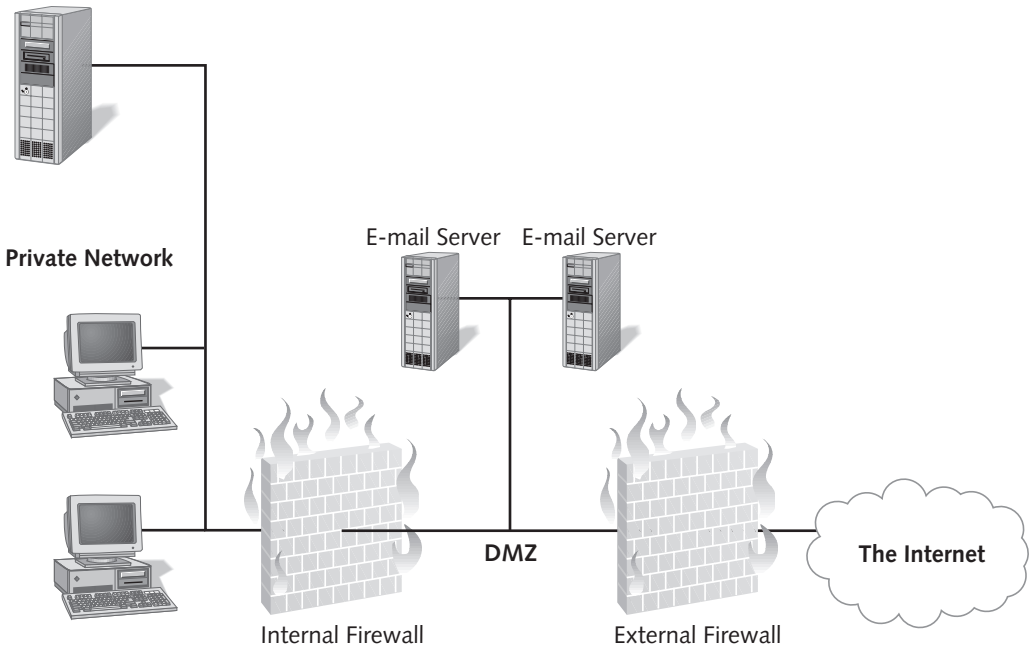


Figure 10-10 A back-to-back DMZ

The advantage to using a back-to-back firewall DMZ is that the use of two firewalls provides extra protection for the internal network. If an attacker breaches the external firewall, the internal firewall will still protect the corporate network. As an added security measure, many companies will implement two different firewall products. This may increase security as two different methods of attack will be needed to reach the internal network.

When you are planning the IP addressing design for the back-to-back DMZ, the internal network and DMZ will be two separate network segments. The DMZ can use either private or public IP addresses, but, as discussed previously, if you are using IPSec to connect from the Internet to a server within the DMZ, public addresses will be needed.

Securing User Access to the Internet

Another important aspect to designing security around an Internet connection is providing secure access to the Internet for the users inside the company. When a company provides user access to the Internet, you have to be prepared for increased threats to the internal network. These risks can decrease security and provide a loss of functionality within the network. Some of the most prevalent risks associated with allowing Internet access are outlined in the next few sections.

Viruses

Users may introduce viruses into the network by receiving e-mail with infected attachments, downloading files, or by accessing Web sites with malicious content. All security plans should include the deployment of a virus scanning application. Virus scanners are usually implemented on the network servers and workstations but should also be installed on the firewall to provide protection at the entrance point of the network.

Unauthorized File Downloads

Users may find various types of software on the Internet, such as games or utilities, that they may download and install on company workstations. Some utilities and applications have been known to cause incompatibility problems in certain situations and configurations. There have also been many cases where virus-infected files have been downloaded and executed within the internal network. Another concern with downloading and installing applications from the Internet is the threat of installing a **Trojan Horse** application. A Trojan Horse application is an application that appears innocent, but may be running malicious code in the background. For example, the game that you download and install may include code that captures all your keystrokes and sends them to an Internet address.

Another common problem is when advanced users install the latest software drivers for attached devices, only to cause an incompatibility with other configurations on the computer system. To prevent unauthorized downloading of files, Windows 2000 allows administrators to restrict users to being able to write data only to their personal profile directory. This can be accomplished by applying the appropriate security template as part of the security policy of the computer. A security policy can also be applied that restricts users from being able to install device drivers on their Windows 2000 workstation.

Bypassing Security Using Personal Modems

In most cases, the firewall is set up to ensure that there is only one entrance point to the network from the Internet. However, with the use of personal modems, users can bypass the corporate security measures and create a risk to the internal network. For example, many users use laptops which are typically equipped with built-in modems. A user may decide to use the modem from their office and dial up to a personal Internet account to check her e-mail. She may not realize that, while the connection is active, there is absolutely no protection from Internet attacks as all DMZ and firewall protection has been bypassed. Strict policies must be put into place to discourage the use of modems within the internal network. For highly secure networks, a security template can be deployed that disables the Remote Access Connection Manager and prevents the use of dial-up networking.

Unauthorized Access to Nonbusiness Internet Content

Another Internet-related security risk is the risk of users accessing inappropriate content on the Internet. As anyone who has ever spent time browsing the Internet knows, the type of content available on the Internet is virtually unlimited, ranging from extremely useful to offensive to most users. With such a variety of information on the Internet, companies are forced to implement policies that outline what is considered appropriate Internet access within the workplace. Policies should be enforced that prohibit any potentially offensive material from being viewed or stored within the corporate network. Designing Internet usage policies is discussed in greater detail later in the chapter.

Administrators must evaluate and decide on a variety of factors when designing Internet security. The first task is to select which protocols to allow for Internet access. Almost always, the first protocol that everyone is allowed to use is HTTP, but you must consider the security risks when allowing other types of applications such as Internet Messaging, FTP, or Telnet. The second task is to decide on individual user and computer access. Some users need to be able to use certain protocols to access information on the Internet, or they may need to be able to access particular areas of the Internet. Other users may be prohibited from accessing particular Web sites or the Internet during certain time periods.

You have two options to configure these restrictions. One option is to use a service such as a proxy server to restrict protocol or user access in or out of the internal network. The second option is to configure the Internet clients to provide increased security when browsing or accessing Internet resources. The following sections will discuss both of these concepts in more detail.

Implementing Proxy Services

For most companies that need to manage Internet access, the best option is to implement a proxy server. A **proxy server** is a service that can be used to restrict Internet access by user name or group membership, protocol, or Web site address.

If you are using a proxy server to control Internet access, all network clients must be configured to forward Internet requests to a configured proxy server. The proxy server then requests the information from the Internet on behalf of the network clients. The proxy server can also operate as a NAT device. This means that all the internal clients can have private IP Addresses, with only the Internet-compatible IP address configured on the external adapter of the proxy server.

Microsoft provides two applications that can be used to provide proxy services: Microsoft Proxy 2.0 and Internet Security and Acceleration (ISA) Server 2000. Both Microsoft Proxy and ISA Server 2000 provide protection at the application, protocol, and packet levels as users access the Internet.

In addition to providing proxy services, ISA Server 2000 is a powerful firewall application.

The proxy service allows you to have a great deal of control over the access internal users have to the Internet. For example, one option is to configure application-level security. **Application-level security** defines which applications can be used to access the Internet. You can also configure **protocol-level security**, which allows you to configure which protocol users can use to access the Internet. In most cases, you will probably allow all users to use the HTTP protocol to access Web sites on the Internet. However, you may want to block all users from connecting to the Internet using the ICQ protocol and allow only some users to use MSN Messenger. You can configure any combination of protocol filters on the proxy server.

You can also control which sites users can access by configuring site or content filters. For example, you may want to allow the use of HTTP to connect to the Internet, but you may want to restrict which Web sites the users can access. You can configure this in one of two ways. In most cases, you will configure the content filter to allow access to all web sites except for the sites that you have explicitly blocked. In other cases, you may want to configure the content filter to deny access to all Web sites except for the ones where you have explicitly granted access.

In addition to restricting access by individual user accounts, proxy services also allow restrictions based upon group memberships. For example, you may configure the proxy server to allow only one Active Directory security group access to a particular chat site. Any user that is not a member of the development group will not be able to access this site.

Another important feature of Microsoft Proxy 2.0 and ISA Server is the generation of detailed logs and reports that can assist in monitoring and auditing Internet usage. If you implement auditing on the proxy server, you must be sure to check the logs and reports regularly to ensure that all Internet policy rules are being followed and to discover any possible security breaches.

Configuring Internet Clients

In addition to implementing proxy services, security policies can also be enforced by configuring individual client settings. Most client settings are configured in the advanced configuration features of the Internet Explorer browser. The security features that are included with Internet Explorer include:

- Security zones
- Content Advisor
- Proxy client configurations

Security Zones

Internet Explorer classifies all web sites into **security zones**. A security zone is then assigned a specific security level. Based upon the Web site IP Address, a site may be assigned to any one of four zones. The four zones include:

- Internet zone—Contains Web sites not assigned to any other zone. The default security level is Medium, which provides most Web browser functionality but will not allow the downloading of unsigned ActiveX applets and prompts the user before downloading potentially unsafe content. The interface to configure the security for this zone is shown in Figure 10-11.

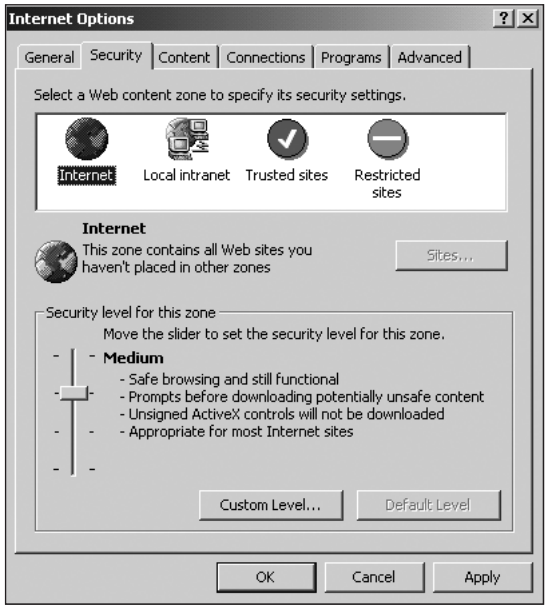


Figure 10-11 Configuring the Internet zone security

- Local intranet zone—Configured for all sites located within the internal network. As shown in Figure 10-12, the default security level is Medium-low, which provides the same basic security as Medium, but will not prompt the user before downloading content from a Web server.

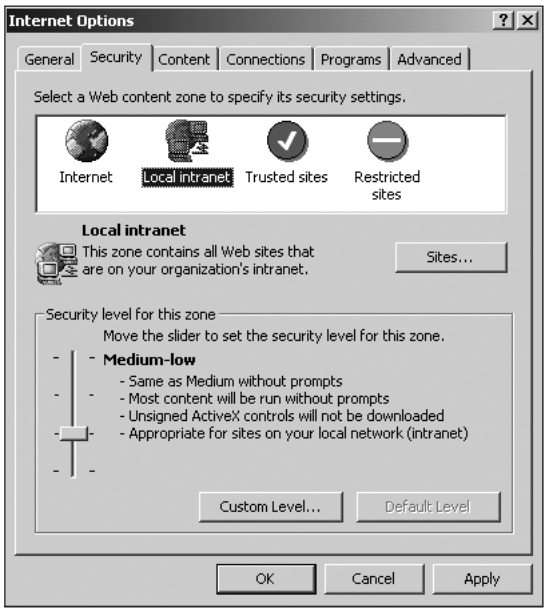


Figure 10-12 Configuring the Local intranet zone security

- Trusted sites—Includes all sites on the Internet that are considered safe for accessing and downloading content. By default, there are no sites assigned to this zone, but you can manually specify which sites are considered trusted. As shown in Figure 10-13, the default security level is Low, which does not provide any security to downloaded or active content.
- Restricted sites—Includes sites that are considered unsafe and a potential security threat. By default, there are no sites assigned to this zone, but you can manually specify which sites are considered untrustworthy. The default security level is High, which provides the least amount of functionality because most features are disabled, such as downloading or accessing active content. Figure 10-14 shows the security setting for this zone.

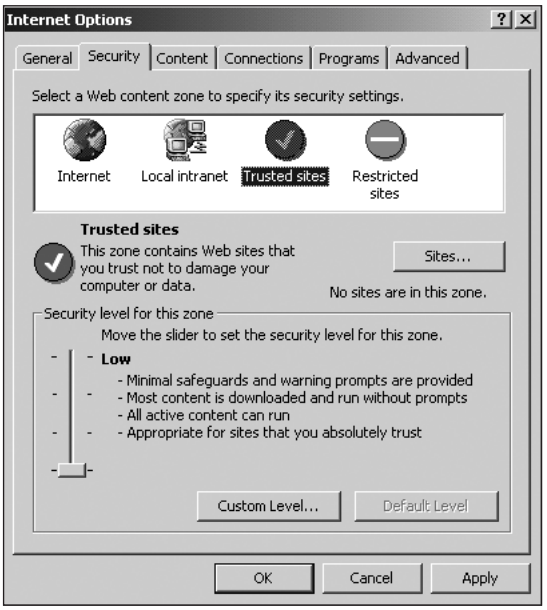


Figure 10-13 Configuring the Trusted sites zone security

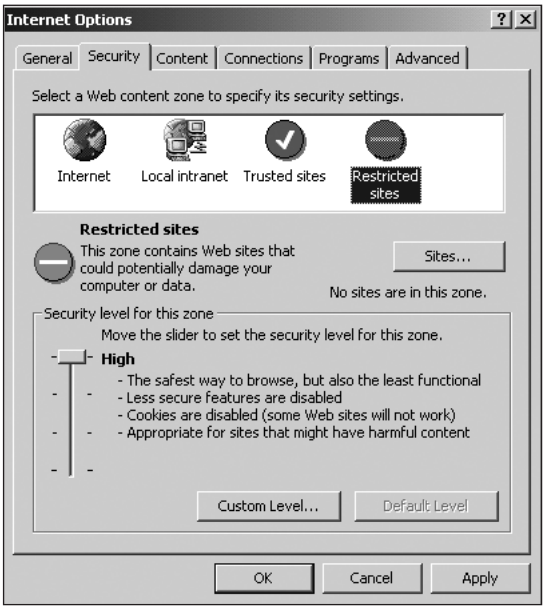


Figure 10-14 Configuring the Restricted sites zone security

To edit zone memberships or security settings follow the procedure below:

1. Open the Internet Explorer Web browser.
2. Click **Tools**, and click **Internet Options**.
3. Click the **Security** Tab. From this tab, you can configure the security settings for each zone, as well as add Web sites to the Restricted or Trusted zones.

The Content Advisor

The **Internet Explorer Content Advisor** can be used to control the types of Web content that users can access. Internet Explorer is installed with the **Recreational Software Advisory Council on the Internet (RSACi)** filter system. The RSACi has organized Internet content into four category levels:

- Language
- Nudity
- Sex
- Violence

As users access Web pages, the Content Advisor screens Web content by reading RSACi ratings embedded in the HTML Meta tags. Based upon the suitability levels configured for each category in the Web browser, the user is either allowed or denied access.

To access the Content Advisor, follow the steps below:

1. Open the Internet Explorer Web browser.
2. Click **Tools**, and click **Internet Options**.
3. Click the **Content** Tab.
4. Click the **Enable** button.
5. Select each category and move the slider to the appropriate rating level as shown in Figure 10-15.

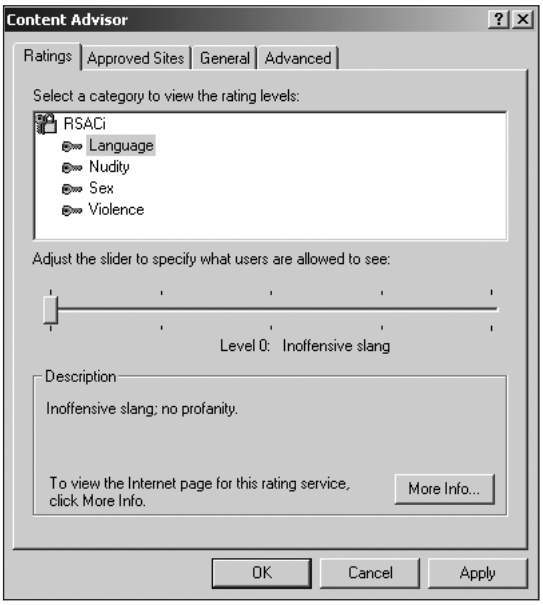


Figure 10-15 Configuring the Internet Explorer Content Advisor

In order for the content filtering in Internet Explorer to be effective, the Web site designer must incorporate the RSACi information in the HTML meta tags for each page. Because very few Web sites actually include this information, the content filtering is ineffective.

Proxy Client Configurations

If you are using a proxy server, all of the client machines need to be configured to use the proxy server whenever they attempt to access Internet resources. To configure the Internet Explorer client, use the following procedure:

1. Open the Internet Explorer Web browser.
2. Click **Tools**, and click **Internet Options**.
3. Click the **Connections** Tab.
4. Click the **LAN Settings** button to view the proxy server configuration settings as shown in Figure 10-16.

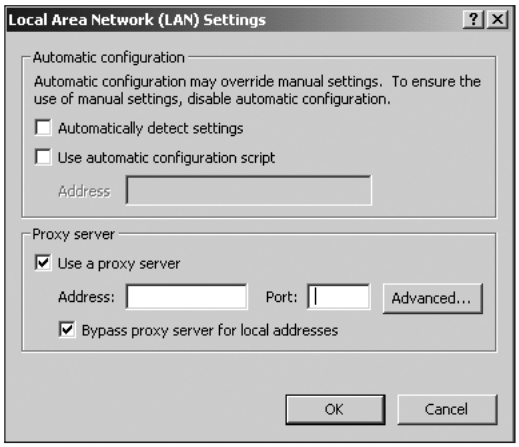


Figure 10-16 Configuring client proxy settings

Internet Explorer allows users to configure and edit their own security settings by accessing the Internet Tools menu. This may not be ideal if an administrator is using these configurations to enforce corporate security policies. The **Internet Explorer Administration Kit (IEAK)** can be used to design customized Web browsers that enforce and lock security and proxy configuration settings.

The Internet Explorer Administration Kit (IEAK) can be downloaded from *http://www.microsoft.com/windows/ieak/techinfo/default.asp.*

Internet Usage Policies

Almost all companies want to set some restrictions on Internet usage. For example, virtually all companies have strict restrictions on the viewing of pornographic information on the Internet. Even if you use the content filtering capability of a proxy server, it may be almost impossible to enforce this restriction just by implementing a technical solution. It is technically impossible to create a content filter list that would block access to all pornographic sites on the Internet, while granting access to all other sites. This situation also requires a corporate policy component.

Most companies have adopted an **Internet usage policy** to deal with such situations. This policy not only states what is acceptable in terms of Internet usage, but it can also serve as a legal contract between the employee and the organization. Before allowing a user to gain Internet access, the company can require that the policy be read and signed to ensure compliance.

An Internet Usage Policy should contain at least the following sections:

- Available services—The first section of the policy should contain descriptions of all approved Internet services that are available to users. Services such as web access and corporate e-mail are examples.
- Acceptable use—The policy must be specific and state which tasks are acceptable when users access the Internet. Specific tasks may include:
  - Users may connect to any web site that relates to business purposes.
  - Users may send and receive e-mail for business purposes.
  - Users may send e-mail attachments that are less that 5 MB in size.
  - Users may download files as long as virus scanners are in place and up-to-date.
  - Users may access only corporate-approved newsgroups.
- Unacceptable use—The policy must specify what is considered unacceptable use when users access the Internet. Some examples of prohibited tasks might include the following:
  - Users may not install unauthorized downloaded software onto their local hard disk.
  - Users may not use the Internet or e-mail for personal use.
  - Users may not access web pages that do not have business purposes, e.g., web sites related to hate, sex, gambling, shopping, or job searching purposes.
  - Users may not install or use internal modems to access the Internet.
  - Users may not expose any confidential business information to people via e-mail or web pages.
- Consequences for violating the usage policy—The usage policy should detail the consequences that will result when an employee breaches the usage policy by performing an unauthorized task. Some consequences might include revoking Internet privileges, employee termination, or legal prosecution.

After the Internet Usage Policy is defined, it should be reviewed by a company lawyer to ensure that the policy is legally binding.

PLANNING BEST PRACTICES

- Be sure to subscribe to the Microsoft Security Notification Services at *http://www.microsoft.com/technet/security/notify.asp*. The security advisor will send automatic notifications of security issues by e-mail. This service is particularly critical for all servers that are accessible from the Internet.

- Check the Microsoft Web site and other Internet security Web sites for any recent security-related tools or white papers. Because the security issues change frequently, the only way to ensure that you are protected from new attacks is to constantly monitor these Web sites. Most Internet security Web sites provide the option to sign up to receive a weekly newsletter detailing security issues, as well as receive critical updates whenever a new security issue has been identified.
- If your network consists of only a few machines, Internet Connection Sharing will be all that is needed to share a single Internet connection. If you need any advanced features, such as DHCP or DNS on your local network, and the network consists of many computers that need Internet access, consider configuring RRAS as a NAT server.
- When designing firewall rules, most security experts suggest denying all packets by default, and only opening ports for protocols that are allowed within the network.
- When designing the corporate network infrastructure, consider implementing a Demilitarized Zone (DMZ) to protect the internal network from the Internet. Place all Internet-accessible resources within the DMZ to allow limited access from the Internet.
- As an added security measure, implement two different firewall products with a back-to-back firewall DMZ. This will increase security as two different methods of attack may be needed to reach the internal network.
- Do not locate domain controllers from the internal network in the DMZ. Install network services on standalone servers, or configure a domain controller as part of a separate forest within the Demilitarized Zone.
- Stop all nonessential services on computers located within the DMZ.
- Use the Internet Explorer Administration Kit to configure and lock down all client-based Internet browser settings.
- For legal protection, be sure to design, implement, and have all users sign an Internet Usage Policy document.

Chapter Summary

- There are two concerns when designing secure access to the Internet. The first concern involves securing the internal network from Internet-based attacks through the use of NAT, firewall configurations, or Demilitarized Zones. The second concern involves securing access to the Internet from within the network by utilizing tools such as Microsoft Proxy or ISA Server 2000.
- Any network service or component that connects to the Internet must be maintained by ensuring that all updated service and security patches have been applied.

- Windows 2000 includes two components that provide NAT services to enable secure Internet access. Internet Connection Sharing can be used in small and simple network environments. RRAS can be configured as an advanced NAT server, which also allows DHCP configuration options and advanced monitoring.
- Firewalls offer a variety of features to assist in increasing the security of the internal network. Some of these features include NAT, packet filter capabilities, Reverse Proxy (static) mappings, usage report statistics, and intrusion detection.
- A common approach to protecting the internal network is to create a protected area between the internal network and the Internet by using firewalls. This protected area is known as a Demilitarized Zone (DMZ) or screened subnet.
- Two design strategies on planning the use of a DMZ include configuring a three-homed firewall DMZ, or configuring a back-to-back DMZ. A three-homed firewall DMZ includes a single firewall connected to three separate network segments. A back-to-back DMZ implements two firewalls, with one firewall between the internal network and the DMZ, and the other firewall between the DMZ and the Internet.
- Some of the most prevalent risks associated with allowing Internet access include viruses, unauthorized file downloads, and access to nonbusiness-related content.
- To assist in controlling and auditing user access to the Internet, implement a proxy service such as Microsoft Proxy 2.0 or ISA Server 2000.
- Internet security can also be configured on the client side. Internet Explorer includes various security features, such as security zones and the content advisor.
- Internet Usage Policies should be created and adopted within the corporation to ensure that appropriate Internet usage is maintained and understood by users.

KEY TERMS

back-to-back DMZ — Two firewalls used to create a protected network segment between the internal network and the Internet.

Demilitarized Zone (DMZ) (screened subnet) — A protected area between the internal network and the Internet, separated by firewalls. Internet-accessible resources are placed within this protected area to keep a distinct separation from the internal network.

firewall — A software-based or hardware-based component that allows only specific types of traffic in or out of the internal network.

firewall rule — The combination of multiple packet filters configured on a firewall.

Internet Connection Sharing (ICS) — A Windows 2000 component which allows the sharing of a single Internet connection to multiple workstations within a network. Usually implemented in a small and simple network where a Windows 2000 Professional or member server is configured to share a single connection to the Internet.

Internet Explorer Administration Kit (IEAK) — Can be used to design customized Web browser implementations that enforce and lock security and proxy configuration settings.

Internet Explorer Content Advisor — Can be used to control the types of Web content that users can access.

Network Address Translation (NAT) — Protects a network by replacing the source internal address and ports of all outgoing packets with a single public IP address.

packet filter — Describes various characteristics of a network packet that define whether the packet will be allowed or denied access through a firewall.

proxy server — A service that can restrict Internet access by user name or group membership, protocol, or by Web site address.

Request for Comment (RFC) 1918 — States that certain IP Addressing ranges have been designated as private. The private IP address ranges include 10.0.0.0–10.255.255.255, 172.16.0.0–172.31.255.255, and 192.168.0.0–192.168.255.255.

reverse proxy (static) mappings — Configuration settings that direct incoming traffic to a particular resource protected behind the firewall.

security zones — One of four classifications used in Internet Explorer to assign security levels to web sites. The four classifications are the Local Intranet zone, Internet zone, Trusted Sites zone, and the Restricted Sites zone.

three-homed firewall DMZ — A DMZ configuration where a single firewall is set up with one network adapter connected to the Internet, a second adapter connected to the private network, and a third adapter connected to the DMZ.

Review Questions

1. To help ensure the security of servers that are accessible from the Internet, you should:
   a. disable all services that are not required on the servers
   b. install the security patches available from Microsoft
   c. install the servers only on NTFS partitions
   d. all of the above
2. What type of network service allows users to access the Internet while using IP addresses defined for internal use only?
   a. packet filtering
   b. proxy server
   c. NAT
   d. RRAS

3. What type of network service usually incorporates caching to speed up access to the Internet?
   a. packet filtering
   b. proxy server
   c. NAT
   d. firewall
4. Which of the following is not a private IP address as discussed in RFC 1918?
   a. 10.50.50.6
   b. 192.168.40.50
   c. 172.35.60.21
   d. 10.200.40.50
5. Which Internet-based threat does not normally damage data, but stops legitimate users from accessing resources?
   a. denial-of-service attacks
   b. unsigned ActiveX controls
   c. executable e-mail attachments
   d. e-mail scripting viruses
6. You have configured Windows 2000 as a NAT server for your network. Now when clients from your network connect to a Web server on the Internet, the Web server will respond to:
   a. the IP address of the client making the request
   b. the IP address of the internal network card on your NAT server
   c. a private IP address
   d. the public IP address on the NAT server
7. When you configure your network for Internet Connection Sharing, you must:
   a. configure the ICS server with any private IP address
   b. configure all the clients to use static IP addresses
   c. allow the ICS installation process to set your IP address
   d. configure all clients to use DHCP
8. Which of the following is not an advantage of NAT configured through RRAS over the ICS version of NAT?
   a. You can install the RRAS NAT on Windows 2000 Professional.
   b. You can use an internal DHCP server.
   c. You can have multiple subnets on your internal network.
   d. You can configure packet filtering on the NAT server.

9. A firewall rule:
   a. explains how the firewall should be configured
   b. configures the NAT process on a firewall
   c. defines what type of traffic will be allowed through a firewall
   d. defines the firewall's IP addresses
10. To ensure that your firewall is as secure as possible, the last firewall rule to be evaluated should allow all traffic that has not been explicitly blocked. True or false?
11. A demilitarized zone (DMZ) is:
   a. a network segment separated by a router from your internal network
   b. a network segment separated by a firewall from your internal network
   c. a network segment directly accessible from the Internet
   d. a network segment separated by a firewall from the Internet
12. To maximize the security of a back-to-back firewall, you should deploy:
   a. only one firewall but make sure it is the best firewall available
   b. two firewalls of the same type
   c. two firewalls to protect the DMZ
   d. two firewalls of different types
13. To prevent users from accessing nonbusiness-related Web sites, you will need to:
   a. Configure a proxy server to block access to some Web sites.
   b. Configure each client to prevent access to some Web sites.
   c. Create and enforce an Internet usage policy.
   d. Disconnect Internet access during working hours.
14. By using a proxy server such as Microsoft Internet Security and Acceleration Server, you can limit user access to the Internet based on:
   a. user
   b. Active Directory security groups
   c. protocol
   d. Web site
   e. all of the above
15. Internet Web sites are added to the Restricted Sites in Internet Explorer when:
   a. a user manually adds them to the list
   b. a user downloads a virus from the site
   c. the site contains nudity
   d. the user downloads a Trojan Horse application from the site

16. An Internet usage policy should define:
    a. each Web site that users are allowed to visit
    b. the protocols users are allowed to use to connect to the Internet
    c. which types of Web sites are not acceptable for viewing
    d. the consequences of inappropriate use of the Internet
    e. all of the above

HANDS-ON PROJECTS

Project 10-1

In this hands-on project, you will configure Routing and Remote Access as a Network Address Translation server.

To uninstall all previous RRAS configurations:

1. Log on to your Windows 2000 computer with an administrator account.
2. Click **Start**, point to **Programs**, point to **Administrative Tools**, and click **Routing and Remote Access**.
3. Right-click your server and click **Disable Routing and Remote Access**.
4. Click **Yes**.
5. To configure a NAT server, right-click the server name or choose **Action** and choose **Configure and Enable Routing and Remote Access**.
6. Click **Next** at the RRAS Wizard welcome screen to view the common configurations of RRAS.
7. To configure the NAT options, choose **Internet connection server** and click **Next**.
8. Choose **Set up a router with the Network Address Translation (NAT) protocol**. Click **Next**.
9. Choose the **External** network interface as the Internet connection.
10. Click **Next**, and then click **Finish**.
11. Continue to the next project.

Project 10-2

In this hands-on project, you will configure various settings on the NAT server to ensure that it is properly configured.

To verify network interface assignment:

1. Expand the **IP Routing** node in the left pane.

2. Select the **Network Address Translation (NAT)** node.
3. In the rightmost pane, right-click the External interface. Click **Properties**.
4. Ensure that the External interface is configured with the **Public interface connected to the Internet** setting. Click **OK**.

To configure DHCP and DNS:

5. In the left pane, right-click **Network Address Translation (NAT)**. Click **Properties**.
6. Click the **Address Assignment** tab.
7. To automatically assign computers IP addresses, select the check box next to **Automatically assign IP addresses by using DHCP**. Leave the default IP address range.
8. To ensure that clients get DNS settings, click the **Name Resolution** tab.
9. Select the check box next to **Clients using Domain Name System (DNS)**.
10. Click **OK**.
11. To uninstall all previous RRAS configurations, right-click your server and click **Disable Routing and Remote Access**.
12. Click **Yes**.
13. Close all windows and log off.

Project 10-3

In this hands-on project, you will secure a client web browser by configuring security zones.

To configure security zones:

1. Log on to your computer with an account that has administrative permissions.
2. Open the Internet Explorer Web browser from the Programs menu or shortcut icon.
3. In the Internet Explorer browser, click the **Tools** menu, and click **Internet Options**.
4. Click the **Security** tab. This is where the four security zones can be configured.
5. You decide to organize known sites into specific zones. Your goal is to place partner sites within the trusted sites zones and a couple of unauthorized

download sites within the Restricted sites zone. The sites to be categorized are listed in the table below:

Trusted Sites	Unauthorized Sites
www.course.com	www.downloads.com
www.imaginets.com	www.mp3.com
www.microsoft.com	www.tucows.com

Place each site into its appropriate zone by selecting the appropriate zone and clicking the **Sites** button. Click **OK** when finished.

6. If connected to the Internet, test each Web site listed above. Notice the zone icon at the lower-right corner of the Web browser.
7. Continue with the next project.

Project 10-4

In this hands-on project, you will secure a client Web browser by configuring the Content Advisor.

To configure the Content Advisor:

1. In the Internet Explorer browser, click the **Tools** menu and click **Internet Options**.
2. Click the **Content** tab and click the **Enable** button.
3. You want to ensure that no site with content that deals with sex or nudity can be viewed. On the **Ratings** tab, select the **Nudity** category and move the slider to level **4**.
4. Select the **Sex** category and move the slider to level **4**. Click **OK**.
5. At the password prompt, type the word **password**. This is the password that protects the configuration so that only people who know the password can edit the settings.
6. Click **OK** on the Content Advisor prompt.
7. If connected to the Internet, test various web sites to see how the Content Advisor works. For Web sites that you want to allow, type the supervisor password at the prompt.
8. To disable the Content Advisor, in the Internet Explorer browser, click the **Tools** menu, and click **Internet Options**.
9. Click the **Content** tab and click the **Disable** button.
10. Type the supervisor password and click **OK**.
11. Click **OK** at the Content Advisor prompt.
12. Close all windows and log off.

CASE PROJECTS

Case Project 10-1

All of the users at Southdale Property Management have access to the Internet. At this point, that Internet access is provided through a 256 Kbps Fractional T1 line that is also used by people on the Internet to access the corporate Web site. The company is using an older router and firewall to provide access to the Internet and protect the internal network. The users are complaining that the access to the Internet is too slow, and management is concerned about the security of the current connection. In addition, the management is very concerned about spending any more money at this time. The cost of upgrading the network to Windows 2000 has strictly limited the amount of money you can spend to resolve this problem. How could you address these concerns?

Case Project 10-2

At this point, all users at Fleetwood Credit Union have access to the Internet through the T1 line at head office. The T1 line is also used by clients accessing the corporate Web site, which is hosted on a Windows 2000 server on the internal network at head office. The management is concerned about the security of the current configuration. It is absolutely critical that the Internet connection be secure and that the Web server also be secure. Ideally, if the Web server is attacked, and someone gains access to the server, the attacker should not have access to the internal network and should also not have access to critical information. How can you ensure the security of the Internet connection and the Web server?